



Safety

SAFETY RULES FOR THE AIRBORNE LAUNCH CONTROL SYSTEM

NOTICE: This publication is available digitally. Contact your Publishing Distribution Office (PDO) for the monthly CD-ROM or access to the bulletin board system. The target date for discontinuing paper publications is December, 1996

This instruction implements AFI 91-1, *Nuclear Weapons and Systems Surety*. It applies to all operations involving the Airborne Launch Control System (ALCS). It assigns responsibilities and gives the system safety rules. The safety rules in this instruction may only be changed using procedures in AFI 91-102, *Nuclear Weapon System Safety Studies, Operational Safety Reviews, and Safety Rules*.

SUMMARY OF REVISIONS

★Deleted "Common" from the name of AFI 91-117 and changed all references to "CALCS" to "ALCS." Prohibited a certified Missile Combat Crewmembers-Airborne (MCCM-A) from USCAS-401 custodial duties or handling responsibilities. Prohibited non-alert aircraft that are uploaded with complete operational cryptovariable data from taking off unless operational Positive Control Material are aboard.

Section A —Authority, Limitations, and Responsibilities

★1. **Joint Chiefs of Staff (JCS) Direction.** The JCS direct the Commander in Chief, US Strategic Command, and Chief of Staff, US Air Force, to implement the safety rules.

2. **Temporary Limitations.** The Air Force may impose restrictions on application of safety rules.

3. Functional Responsibilities:

3.1. Commander, Air Force Safety Agency:

- Ensures that the safety rules work, providing maximum safety consistent with operational requirements.
- Ensures that units follow the safety rules.

3.2. Using Commands:

- Ensure that their units follow the safety rules.
- Ensure that all safety standards and procedures agree with the approved safety rules.
- Inspect for compliance.

3.3. Air Force Materiel Command (AFMC). AFMC ensures that its manuals, checklists, and technical orders do not conflict with the safety rules.

Section B —Safety Rules

4. General Guidance:

4.1. Safety rules always apply, even during war.

Supersedes: AFI 91-117, 18 March 1994.
OPR: HQ AFSC/SEWN (Lt Col Warren R. Adams)

Certified by: HQ USAF/SE (Brig Gen Orin L. Godsey)
Pages: 4/Distribution: F

4.2. A commander may deviate from a specific rule in an emergency but may not expend a nuclear weapon until authorized by an emergency war order. DoD Directive 3150.2, *Safety Studies and Review of Nuclear Weapon Systems*, February 8, 1984, defines an emergency as “an unexpected occurrence or set of unexpected circumstances in which personnel or equipment unavailability due to accident, natural event, or combat may demand immediate action that may require extraordinary measures to protect, handle, service, transport, or employ a nuclear weapon.”

4.3. These safety rules, weapon system features, operational and administrative controls, and technical procedures ensure that the ALCS meets the Nuclear Weapon System Safety Standards in AFI 91-101, *Air Force Nuclear Weapons Surety Program*, and DoD Directive 3150.2.

5. Security Criteria:

5.1. AFI 31-101, *Air Force Physical Security Program*, and DoD C-5210.41-M, *Nuclear Weapon Security Manual (U)*, apply.

★5.2. When KIK-45 Volatile Keying Assemblies (VKA), A-VKA or B-VKA, are aboard:

- Control access to the aircraft and deny entry to any personnel unless the two Missile Combat Crewmembers-Airborne (MCCM-A) assigned to the aircraft are present. EXCEPTION: Any Two-Person Concept team assigned to the aircraft may enter if the A-VKA and B-VKA are properly secured in the code processor equipment (CPE) or the alarmed container with two approved locks.
- Don't grant unescorted entry to the aircraft to anyone who had access to the Offutt Air Force Base ICBM Code Processing System (ICPS) when current operational ALCS code data was prepared.

6. Tamper Control and Detection. AFI 91-104, *Nuclear Surety Tamper Control and Detection Programs*, defines the Two-Person Concept.

7. Handling and Storage of Critical Components and Certified Software. AFI 91-105, *Critical Components*, applies.

8. Personnel Reliability. AFI 36-2104, *Nuclear Weapons Personnel Reliability Program*, applies.

9. Equipment, Procedures, Checklists, and Modifications:

9.1. Use only equipment, procedures, and checklists that are consistent with publications approved by the US Air Force for any operation directly associated with nuclear weapons, nuclear weapon systems, or the ALCS.

9.2. Make sure the US Air Force has approved all publications and equipment modifications and that the

publications and modifications conform to the safety rules in this instruction and the DoD Nuclear Weapon System Safety Standards.

10. Operational Code Control:

10.1. When putting a ALCS-configured aircraft on alert, successfully complete these test sequences before loading either the operational cryptovariable or the operational S-data:

- Airborne Operational Program Load 1 Crypto Sumcheck (CSC).
- Fail CSC.
- Fail CPE.
- CPE Test.
- Decrypt Test Sequences.

10.2. Reinitiate the preceding tests if any of the following equipment is changed:

- Airborne Launch Control System Controller (ALCSC) processor chassis.
- ALCSC expansion chassis.
- Portable storage unit.
- CPE.

10.3. After electronically loading the cryptovariable data into the CPE, secure the access doors on the CPE with two approved locks to secure the A-VKA and B-VKA and prevent use of the Classified Command Control switch. A single person must not know both combinations or control the keys to both locks.

★10.4. Do not allow a person certified to perform MCCM-A duties to be a USCAS-401 custodian or a member of a USCAS-401 handling team.

10.5. When transferring components between two aircraft in a single Priority A alert aircraft parking area, lock the A-VKA and B-VKA in the CPE with two approved locks. A single person must not know both combinations or control the keys to both locks.

10.6. Don't carry complete operational cryptovariable data aboard an aircraft, except when you have met the provisions of paragraph 11.

10.7. When removing an aircraft from alert, erase the cryptovariable data stored in the CPE by cycling the CPE power switch. Two MCCM-A must witness the lighting of the CPE's AC and BC lights.

10.8. Don't remove VKA covers, except for emergency VKA destruction.

★10.9. If you can't erase the VKA memory, continue to control as an operational VKA until the cryptovariable data stored in memory have been superseded.

★10.10. When non-alert aircraft are uploaded with complete operational cryptovariable data, the aircraft will not take off with operational Positive Control Material aboard.

11. Aircraft Configuration:

11.1. If an operationally coded A-VKA or B-VKA is installed or if operational cryptovariable data are electroni-

cally loaded in the CPE, follow these procedures until two MCCM-A authenticate an execution order:

11.1.1. Keep the ALCC switch in the OFF position, except when conducting authorized tests.

11.1.2. Don't activate the Multifunction Selector ALARM OVERRIDE switch, except when:

- Electronically loading the operational cryptovisible data.
- Unloading operations after removing the operationally coded A-VKA and B-VKA and erasing the electronically loaded operational cryptovisible data.

11.1.3. Don't move the Classified Command Control switch inside the CPE to ENABLE, except when conducting authorized tests.

11.2. Install the operationally coded A-VKA and B-VKA in the CPE and verify the capability of the VKA erase circuits before an ALCS-configured aircraft takes off. Do not preclude aircraft takeoff directed by an emergency war order if the erase circuits fail to verify.

★11.3. Keep the operationally coded A-VKA and B-VKA in the CPE and the selector switches in the ARM position

during takeoff, flight, and landing, except when required for airborne equipment checkout and loading procedures, inflight electronic loading of the cryptovisible data, and/or fault analysis while airborne.

★11.3.1. If the selector switches need to be placed to the SAFE position while airborne, the aircraft must be in level flight at cruise altitude and free of malfunctions that could be dangerous to flight.

★11.3.2. The selector switches need not be returned to the ARM position after two MCCM-A have authenticated an execution order.

★11.3.3. If the VKAs must be removed while airborne, the MCCM-A will maintain proximity to the CPE to facilitate immediate reinstallation and arming of the VKAs if safety-of-flight status changes.

12. Simulated Electronic Launch Test Procedures. For applicable missile system safety rules, consult AFI 91-114, *Safety Rules for Intercontinental Ballistic Missile Weapon Systems*.

ORIN L. GODSEY, Brig General, USAF
Chief of Safety

GLOSSARY OF REFERENCES, ABBREVIATIONS, AND ACRONYMS

References

AFI 91-101, *Air Force Nuclear Weapons Surety Program*
AFI 91-102, *Nuclear Weapon System Safety Studies, Operational Safety Reviews, and Safety Rules.*
AFI 91-104, *Nuclear Surety Tamper Control and Detection Programs*
AFI 91-105, *Critical Components*
AFI 91-114, *Safety Rules for Intercontinental Ballistic Missile Weapon Systems.*
AFI 31-101, *Air Force Physical Security Program*
AFI 36-2104, *Nuclear Weapons Personnel Reliability Program*
DoD Directive 3150.2, *Safety Studies and Reviews of Nuclear Weapons Systems*
DoD C-5210.41-M, *Nuclear Weapon Security Manual (U)*

Abbreviations and Acronyms

AF–Air Force
AFMC–Air Force Material Command
AFI–Air Force Instruction
AFPD–Air Force Policy Directive
AFSC–Air Force Safety Center
ALCS–Airborne Launch Control System
ALCSC–Airborne Launch Control System Controller
CPE–Code Processor Equipment
ICPS–ICBM Code Processing System
JCS–Joint Chiefs of Staff
MCCM-A–Missile Combat Crewmembers-Airborne (MCCM-A)
VKA–Volatile Keying Assemblies